REMARKS

Applicant respectfully requests reconsideration of the present application in view of the reasons that follow.

1.   Claim Rejections – 35 U.S.C. § 102

Claims 1-4, 6-12, 14-17 and 19-20 were rejected under 35 U.S.C. § 102(b) as being anticipated by Bodnar ("Bodnar," U.S. Patent No. 6,061,790). Applicants respectfully traverse the rejection.

Claim 1 is directed to a method of protecting a username during authentication and recites, among other limitations:

> obtaining a plain text username over a secure communication channel; . . .
>
> obscuring the plain text username using the server identifier; . .
>
> communicating authentication information including the obscured username over a non-secure communication channel from a client.

As discussed in the specification, a username or user identification is obscured or encrypted for use in a plain text, unencrypted authentication scheme. See, specification, page 1, paragraph 4. An obscured username or user identification may be created by encrypting a plain text username. See, specification, page 2, paragraph 6. In an exemplary embodiment, a plain text username is provided over a secure channel and then obscured or encrypted. See, specification, page 6, paragraphs 29 and page 7, paragraph 30. Both the obscured username and plain text user name are registered or stored on the server with which the client device will communicate. See, specification, page 5, paragraph 21, page 6, paragraphs 27 and 29 and page 7, paragraph 30. A client device uses the obscured or encrypted username when communicating with the server over a non-encrypted channel. See, specification, page 1, paragraph 4, page 2, paragraph 6, page 4, paragraph 18 and page 5, paragraph 22.

In contrast, Bodnar does not teach, disclose or suggest a method of protecting a username during authentication including obtaining a plain text username over a secure

-2-

communication channel, obscuring the plain text username using the server identifier and communicating authentication information including the obscured username over a non-secure communication channel from a client. Rather, Bodnar teaches a method for establishing a secure communication line between a client and a server. See, Bodnar, Abstract, col. 3, lines 13-20 and col. 3, lines 48-54. A user logs in to a client by entering a user name and password and the client sends a request for a secure session to the server that includes only the user name over an open channel. See, Bodnar, Figure 3, col. 6, lines 14-16 and col. 7, lines 50-53. The client and server then engage in an authentication process in which public key enciphering information is calculated and exchanged in order to establish the secure connection and authenticate the client and server. See, Bodnar, Figure 3, col. 7, lines 22-30, col. 7, line 57 to col. 9, line 35 and col. 9, lines 38-42. Bodnar describes a fingerprint or hash function (calculated using the user password which is not sent to the server) that is prestored on the server and calculated by the client, however, it appears the user name and user ID are transmitted between the client and server without being obscured or encrypted. See, Bodnar, Figure 3, col. 7, lines 57-63, col. 8, lines 11-14, lines 20-28, and lines 51-67, col. 9, lines 9-12 and lines 18-21. Accordingly, claim 1 is believed to be allowable over Bodnar.

Claim 10 is directed to a username protection process and recites, among other limitations:

> registering a user with a selected server . . . creating an obscure
> version of the plain text user identifier, and storing the plain
> text user identifier and the obscure version of the plain text user
> identifier on the selected server; and
>
> initiating a communication session between the user and the
> selected server by the communication of the obscure version of
> the plain text user identifier over a plain text communication
> channel.

Bodnar does not teach, disclose or suggest creating an obscure version of the plain text user identifier, storing the plain text user identifier and the obscure version of the plain text user identifier on the selected server or initiating a communication between the user and the selected server by the communication of the obscure version of the plain text user

identifier over a plain text communication channel. As discussed above with respect to claim 1, Bodnar teaches a method for establishing a secure communication line between a client and a server using public key enciphering. See, Bodnar, Abstract, col. 3, lines 13-20, col. 3, lines 48-54 and col. 7, lines 20-22. Bodnar describes a fingerprint or hash function (calculated using the user password which is not sent to the server) that is prestored on the server and calculated by the client, however, it appears the user name and user ID are transmitted between the client and server without being obscured or encrypted. See, Figure 3, col. 7, lines 57-63, col. 8, lines 11-14, lines 20-28, and lines 51-67, col. 9, lines 9-12 and lines 18-21. Accordingly, claim 10 is believed to be allowable over Bodnar.

Claim 14 is directed to a system for protecting a username during authentication over a non-encrypted channel and recites, among other limitations:

> a server having stored therein a plain text user identifier
> communicated by the client device over a secure
> communication channel and an obscured user identifier
> corresponding to the plain text user identifier.

As discussed above with respect to claim 1, Bodnar does not teach, disclose or suggest a server having a stored a plain text user identifier communicated by the client device over a secure communication channel and an obscured user identifier corresponding to the plain text user identifier. Accordingly, claim 14 is believed to be allowable.

Claims 2-4 and 6-9 depend from independent claim 1 and incorporate the limitations of independent claim 1 and are therefore allowable over Bodnar for, among other reasons, the same reasons as given above with respect to independent claim 1. Claims 11 and 12 depend from independent claim 10 and incorporate the limitations of independent claim 10 and are therefore allowable over Bodnar for, among other reasons, the same reasons as given above with respect to independent claim 10. Claims 15-17, 19 and 20 depend from independent claim 14 and incorporate the limitations of independent claim 14 and are therefore allowable over Bodnar for, among other reasons, the same reasons as given above with respect to independent claim 14.

Accordingly, claims 1-4, 6-12, 14-17 and 19-20 are believed to be allowable. Withdrawal of the rejection under 35 U.S.C. § 102(b) and allowance of claims 1-4, 6-12, 14-17 and 19-20 is respectfully requested.

2.   Claim Rejections – 35 U.S.C. 103

Claims 5 was rejected under 35 U.S.C. § 103(a) as being unpatenable over Bodnar in view of Droge ("Droge," U.S. Published Patent Application No. 2002/004898). Claims 13 and 18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Bodnar in view of Shi et al. ("Shi," U.S. Patent No. 5, 875, 296). Applicants respectfully traverse the rejection. Claim 5 depends from independent claim 1 and incorporates the limitations of independent claim 1 and is therefore allowable over Bodnar in view of Droge for, among other reasons, the same reasons as given above with respect to independent claim 1. Claim 13 depends from independent claim 10 and incorporates the limitations of independent claim 10 and is therefore allowable over Bodnar in view of Shi for, among other reasons, the same reasons as given above with respect to independent claim 10. Claim 18 depends from independent claim 14 and incorporates the limitations of independent claim 14 and is therefore allowable over Bodnar in view of Shi for, among other reasons, the same reasons as given above with respect to independent claim 14.

Accordingly, claims 5, 13 and 18 are believed to be allowable. Withdrawal of the rejection under 35 U.S.C. § 103(a) and allowance of claims 5, 13 and 18 is respectfully requested.

3.   Conclusion

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment,

to Deposit Account No. 06-1447. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 06-1447. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 06-1447.

Respectfully submitted,

Date _____ 10/31/05 _____   By _____ Jean M. Tibbetts _____

FOLEY & LARDNER LLP   Jean M. Tibbetts
777 East Wisconsin Avenue   Attorney for Applicant
Milwaukee, Wisconsin 53202-5306   Registration No. 43,193
Telephone: (414) 297-5531
Facsimile: (414) 297-4900